Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended): A system for providing secure exchange of sensitive information with an implantable medical device, comprising:

a crypto key uniquely associated with an implantable medical device to encrypt sensitive information during a data exchange session; and

an external source, comprising:

a key module configured to securely obtain the crypto key over a secure connection from a secure key repository securely maintaining the crypto [[key,]] key and further configured to encrypt the sensitive information using the crypto [[key,]] key;

a long range transmission module configured to transmit the encrypted sensitive information to the implantable medical device via a long range interface and further configured to store the encrypted sensitive information ~~as encrypted data~~ onto the implantable medical [[device,]] device; and

a short range transmission module configured to further [[store]] transmit a copy of at least a part of the sensitive information to the implantable medical device via a secure short range interface and further configured to store the copy as unencrypted data onto the implantable medical device ~~over a secure connection~~.

2. (currently amended): A system according to Claim 1, ~~further comprising: a~~ wherein the short range interface [[to]] logically ~~define~~ defines a secured area around the implantable medical device within which to securely obtain the crypto ~~key; and a~~ and the long range interface [[to]] logically ~~define~~ defines a non-secured area extending beyond the secured area within which to exchange the encrypted data.

3. (original): A system according to Claim 1, wherein the encrypted data is retrieved from the implantable medical device over a non-secure connection and the encrypted data is decrypted as the sensitive data using the crypto key.

4. (original): A system according to Claim 3, wherein the crypto key is securely retrieved over a secure connection from the secure key repository prior to decrypting the encrypted data.

5. (original): A system according to Claim 3, wherein the encrypted data is retrieved through long range telemetry.

6. (original): A system according to Claim 5, wherein the long range telemetry comprises radio frequency telemetry.

Claim 7 (canceled).

8. (previously presented): A system according to Claim 1, wherein the unencrypted data is securely retrieved from the implantable medical device over a secure connection.

9. (original): A system according to Claim 1, wherein the crypto key is securely retrieved from the secure key repository through a programmer.

10. (original): A system according to Claim 1, wherein the crypto key is maintained on the implantable medical device, and the crypto key is retrieved through short range telemetry.

11. (original): A system according to Claim 10, wherein the short range telemetry comprises inductive telemetry.

12. (original): A system according to Claim 1, wherein the external source comprises at least one of a programmer and a repeater.

13. (original): A system according to Claim 1, wherein the crypto key comprises an encryption key in accordance with the Advanced Encryption Standard.

14. (currently amended): A method for providing secure exchange of sensitive information with an implantable medical device, comprising:

defining a crypto key uniquely associated with an implantable medical device to encrypt sensitive information during a data exchange session;

securely obtaining the crypto key over a secure connection from a secure key repository securely maintaining the crypto key;

encrypting the sensitive information using the crypto key, transmitting the encrypted sensitive information to the implantable medical device via a long range interface, and storing the encrypted sensitive information ~~as encrypted data~~ onto the implantable medical device; and

further ~~storing~~ transmitting a copy of at least a part of the sensitive information to the implantable medical device via a secure short range interface and storing the copy as unencrypted data onto the implantable medical device ~~over a secure connection~~.

15. (original): A method according to Claim 14, further comprising:

logically defining a secured area around the implantable medical device within which to securely obtain the crypto key; and

logically defining a non-secured area extending beyond the secured area within which to exchange the encrypted data.

16. (original): A method according to Claim 14, further comprising:

retrieving the encrypted data from the implantable medical device over a non-secure connection; and

decrypting the encrypted data as the sensitive data using the crypto key.

17. (original): A method according to Claim 16, further comprising:

securely retrieving the crypto key over a secure connection from the secure key repository prior to decrypting the encrypted data.

18. (original): A method according to Claim 16, further comprising:
retrieving the encrypted data through long range telemetry.

19. (original): A method according to Claim 18, wherein the long range telemetry comprises radio frequency telemetry.

Claim 20 (canceled).

21. (currently amended): A method according to ~~Claim 21~~ Claim 14, further comprising:
securely retrieving the unencrypted data from the implantable medical device over a secure connection.

22. (original): A method according to Claim 14, wherein the crypto key is securely retrieved from the secure key repository through a programmer.

23. (original): A method according to Claim 14, further comprising:
maintaining the crypto key on the implantable medical device; and
retrieving the crypto key through short range telemetry.

24. (original): A method according to Claim 23, wherein the short range telemetry comprises inductive telemetry.

25. (original): A method according to Claim 14, wherein the external source comprises at least one of a programmer and a repeater.

26. (original): A method according to Claim 14, wherein the crypto key comprises an encryption key in accordance with the Advanced Encryption Standard.

27. (currently amended): An apparatus for securely transacting a data exchange session with an implantable medical device, comprising:

means for defining a crypto key uniquely associated with an implantable medical device to encrypt sensitive information during a data exchange session;

means for securely obtaining the crypto key over a secure connection from a secure key repository securely maintaining the crypto key;

means for encrypting the sensitive information using the crypto key, means for transmitting the encrypted sensitive information to the implantable medical device via a long range interface, and means for storing the encrypted sensitive information ~~as encrypted data~~ onto the implantable medical device; and

means for further ~~storing~~ transmitting a copy of at least a part of the sensitive information to the implantable medical device via a secure short range interface and means for storing the copy as unencrypted data onto the implantable medical device ~~over a secure connection~~.

28. (currently amended): An implantable medical device for securely maintaining sensitive information, comprising:

an implantable medical device, comprising:

a receiver to receive sensitive information via a long range interface and a copy of at least a part of the sensitive information via a short range interface;

a memory to store the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and ~~at least a part of the sensitive information~~ the copy as unencrypted data; and

a secure interface to provide access to the stored sensitive information exclusively over a secure connection.

29. (currently amended): An method for securely maintaining sensitive information on an implantable medical device, comprising:

receiving sensitive information via a long range interface and a copy of at least a part of the sensitive information via a short range interface;

storing the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and ~~at least a part of the sensitive information~~ the copy as unencrypted data; and

providing access to the stored sensitive information exclusively over a secure connection.

30. (currently amended): An apparatus for securely maintaining sensitive information on an implantable medical device, comprising:

means for receiving sensitive information via a long range interface and a copy of at least a part of the sensitive information via a short range interface;

means for storing the sensitive information encrypted using a crypto key uniquely associated with an implantable medical device and ~~at least a part of the sensitive information~~ the copy as unencrypted data; and

means for providing access to the stored sensitive information exclusively over a secure connection.